

REMEDIES FOR TELECOM RECOVERY

NETWORK RESILIENCY

**Report of the Advisory Committee
On
Network Resiliency**

**THE FOLLOWING REPORT SUMMARIZES THE
WORK OF THE ADVISORY COMMITTEE. IT ONLY REFLECTS
THE AUTHOR'S VIEWS AND DOES NOT
NECESSARILY REFLECT THE VIEWS OF CITI OR
THE INDIVIDUAL MEMBERS OF THE
ADVISORY COMMITTEE**

Resilient Networks Module

Final Report Summary

CITI, Columbia Business School

The purpose of this module has been to consider how the study of resilient networks can lead to concrete recommendations to guide government agencies at various levels, industry groups and customers as well as companies involved in critical areas of the telecommunications, internet and related businesses. We pay particular attention to the underlying issue of the current downturn in the telecommunications industry and pose the questions: will resiliency concerns become a drag on the industry, or might they provide a stimulus that helps to revive investment as well as business quality?

Introduction

The issue of network resilience has always been a concern at the intersection of design, engineering and maintenance, of business practice and of standards setting and regulation. Although by most measures the networks have been getting increasingly resilient, with the breakup of the Bell System new responsibilities were assumed in a competitive commercial environment. Increasingly resilience and reliability are variously regarded as a matter of industry technical standards, outage reporting routines, and marketplace competition in the context of customer churn.

Our current situation is one of increasing anxiety about the fragility of our communication networks just as market downturn and national security worries coincide to make the solutions both more urgent and less easy to afford. A number of institutions are addressing engineering approaches to these problems, including our own Columbia University Center for Resilient Networks [www.crn.columbia.edu], but few independent bodies have investigated the business, economic and policy aspects of these necessary changes.

Our goal, through this module as well as the associated research activities in the Columbia Institute for Tele-Information, is to show what business strategies and government policies are most likely to foster improved network resiliency. In this report we provide recommendations that will address key issues such as the role of the Internet in assuring resiliency, the commercial potential of competing forms of network access and especially emerging wireless technologies, the extent to which government involvement will be necessary in the short term (and perhaps continued funding over the longer term), and how greater communications functionality can be achieved for emergency service workers in systems based on commercialized technologies.

The Workshops

The first workshop addressed four substantive issues: 1) the effects of the economic downturn, 2) changing customer expectations, 3) competition and collaboration, and 4) managing interconnection. The starting points for discussion are described below:

1) The effects of the economic downturn on resilience and the generation of new solutions

Before much progress will be made in determining what technical solutions can be implemented, we must address the questions, “who will pay, and how much?” We also have to have an idea of what justifies investment in improving the infrastructure, especially where government funds are involved. To crystallize this problem, I offer three simple scenarios for the impact of network resiliency concerns on telecom recovery:

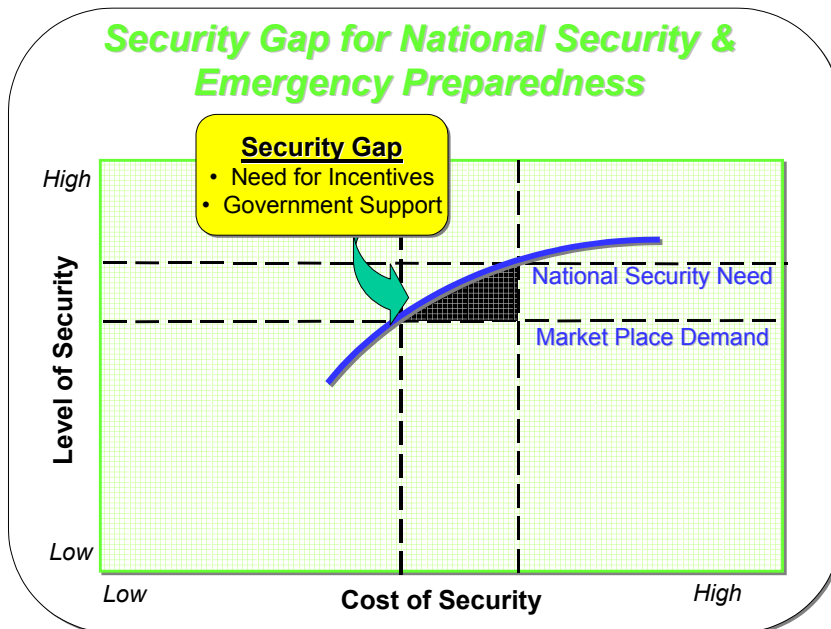
a) Status quo: The telecom slump continues; government does not finance infrastructure improvement; the industry fails (or is not allowed) to consolidate:

In this scenario network resiliency becomes interpreted as emergency preparedness and governments concentrate on special network functionality such as the Government Emergency Telecommunication System [GETS] and some civilian applications of existing military technology under the aegis of the Department of Homeland Security. State and local government are expected to ensure the functioning of emergency services with no major changes in technology. Major corporate customers concentrate on ensuring business continuity internally and on an ad-hoc basis in conjunction with their telecoms services provider(s). No significant investment is made to help the industry out of slump or even to stimulate new businesses in specialized technologies.

b) Private sector stimulus: Network resiliency is identified as a business priority; a greater diversity of services is encouraged through customer take-up of wireless LAN technologies; small firms proliferate to offer terminal equipment, services, content and to pioneer new technologies; these firms prosper as they attract investment from ILECs invigorated by consolidation and the end of price wars.

This optimistic scenario supposes that a market emerges for increased resilience, perhaps stimulated by the largest consumers (in the financial services business, retailing, logistics and government) some of whom have already shown they are willing to pay for premium services themselves and perhaps indirectly stimulate the research and investment needed to upgrade resilience more generally. Conflicts will arise from the accelerated take-up of 802.11b-type wireless technologies and their challenge to ILECs, but the wireless LAN business prospers perhaps through Cisco/IBM-type sponsorship, perhaps reluctantly financed by ILECs that fear being sidelined in the new market. This scenario presumes that destructive competition and price wars end soon with consolidation and the emergence of perhaps 3-4 national carriers and fewer than 4 local service providers in any area. It also presumes that the entire network is made more resilient by cooperation among national and local service providers of all types of technology.

c) Government stimulus: Provisions such as mandatory excess capacity of license holders are financed from the federal budget; the fragility of the Internet is seen as a problem of national significance, attracting major funding to make it more secure; military and special emergency application technologies are aggressively transferred to civilian use, perhaps on the model of the aerospace industry; spectrum use is radically transformed. Some of this is nicely expressed in the chart below, from a recent NRIC report (NIRC VI Homeland Security Working Group on Physical Security Report, Dec. 2002, p. 46; with thanks to Karl Rauscher):



2) *Changing expectations among customers for reliability and resilience*

Perhaps the most important force to emerge driving resilience forward will be the increasing expectations that customers define. Regardless of the scenario above, there is both a strongly felt popular need for “total” reliability and increasing pressure from industry and government agencies that business reliability be better ensured through network improvements. This is evident in the recently published Government Accounting Office report: “Potential Terrorist Attacks; additional actions needed to better prepare critical financial markets participants” GAO Report to the Committee on Financial Services, House of Representatives, GAO-03-414 and available at <http://www.gao.gov/new.items/d03414.pdf>.

A similar perspective is available from the Security and Exchange Commission’s recent “Draft Interagency White Paper on Sound Practices to Strengthen the Resilience of the U.S. Financial System” [Release No. 34-46432; File No. S7-32-02 and available at <http://www.sec.gov/rules/concept/34-46432.htm>]. See also the response of the Securities Industry Association available at <http://www.compitello.com/SIAWhitePaper10-21-02.pdf>.

3) *Competition and collaboration to accommodate emergencies*

At the core of concerns about the workability of various mutual aid and restoration schemes (as shown in the experiences of the New York City MARC) is the question of the extent to which competition inhibits the effective implementation of collaboration, even in emergencies. Although we may feel encouraged by the excellent response as a result of the 9-11 attack on the World Trade Center, we might draw the lesson that this was a unique reaction to unprecedented and dramatic destruction. The common experience of mutual aid has been one of hampered effectiveness due to competition concerns that inhibited detailed forward planning and complicated the means to share critical information about network architecture as well as customers.

4) Interconnection and making collaboration happen

This theme lies at the very heart of the problem of designing and managing the resilient network of the future. I list the theme here mainly to mark our continuing concern with the larger set of issues and the presumption that increasing interconnection will occur, that it will be a force for greater resilience, and that by its very nature it provides some of the most difficult challenges to business strategy as well as government policy.

The purpose of the second workshop was to consider how the study of resilient networks can lead to concrete recommendations to guide government agencies at various levels, industry groups and customers as well as companies involved in critical areas of the telecommunications, internet and related businesses. This led to the consideration of the following recommendations.

1. Encourage inter-modal competition by fostering development and experimentation with new resilient technologies and architectures.
2. Stimulate demand by raising standards for business continuity and communications security.
3. Subsidize new network architecture technologies that promote high capacity and flexibility, especially with regard to wireless and IP technologies.
4. Reassess governmental roles to reflect national security priorities in building out and using communications networks in the manner commonly applied to assure spare capacity in transportation infrastructure.

Categorizing the problem

Improvements in resiliency can be seen to emerge from changes in the industry generally—that is, either the continuation of current trends or the application of recommendations broadly agreed upon by observers of the industry. However, there is also a broad category of recommendations that emerges from specific resiliency concerns, such as the promotion of particular technologies and direct subsidies (from government or through charges to customers). We address the first only briefly because issues such as spectrum reform and competition policy, while of great importance to resiliency, have long been separate areas of debate. While we can show the importance of appropriately resolving these issues, we feel that our major contributions will come from our understanding of new problems and opportunities associated with resiliency.

Five problem areas associated with resilience:

Congestion: the overloading of pathways, especially in emergencies such that traffic must be rerouted. Denial of service attackers generally use congestion maliciously to overload pathways.

Collaboration and interconnection: the ability to share resources and alter routes and modes. In emergencies and in times of serious congestion mutual aid agreements must be made to work and to accommodate inter-modal communications.

Physical resilience: protecting facilities from damage; including central stations, conduits, towers, airwaves, etc. Ensure communications and business continuity through distributed facilities and shared capabilities to minimize the effects of physical damage.

Security: ensuring that routes, messages, procedures, equipment, etc. are safeguarded from intrusion, tampering, distortion, etc.

Emergency response: immediate patching of damage, rerouting of traffic, and new approaches to communications for emergency workers and those caught up in crises that take into consideration both effective transmission capabilities and appropriate content to inform those involved.

Summary of recommendations

- Ensure inter-modal competition
- Stimulate demand for resiliency by raising standards
- Subsidies to build out critical infrastructure
- Devise new governmental roles and priorities, e.g. support spare capacity

1) Maintain inter-modal competition in balance with consolidation. No one system is invulnerable but layers of networks create options, as we currently have in many areas where wireless local area networks, cable modem, personal communication devices, emergency communications systems, mobile telephones, and even powerline communications systems exist alongside wireline plain old telephone systems. This will allow a spread in facilities and avoid the problems associated with, for example, excessive and sometimes uncharted confluence of conduits. We should also encourage moves towards enabling functionality at the network edge (and “dumb pipes”) to open networks more and to do this through alliances rather than vertical integration strategies. This is likely to foster solutions such as VoIP and stimulate business and investment, possibly at the cost of traditional wireline service providers. This implies that regulators allow for the imaginative use of spectrum and other delivery mechanisms (we welcome, for example, the recent FCC statements encouraging powerline communications developments) and that competition policies be reassessed to allow for and encourage companies to plan for coordination. We would also wish to see stimulation through experiments sponsored by large users, property developers, local communities, etc. This helps to address elements of all five problem areas associated with resilience.

2) Stimulate demand by raising standards for business continuity and communications security. Some mechanisms are straightforward and will attract relatively little objection, such as encouraging best practices for data protection and back-up in critical industries. This could be done with industry cooperation through bodies such as the Securities Industry Association and regulators including the Securities & Exchange Commission, the Treasury and the Federal Banking system. Precedents exist in recommendations for business continuity, and we can learn from the Y2K software improvement campaign. A targeted awareness campaign, bringing together Federal, state and in some places local

authorities could educate major commercial customers in all sectors about the value of raising resiliency standards. Governmental bodies would also stimulate demand as they improve the resiliency of their use of networks and local authorities should speed up the deployment of E-911 facilities. In the medium term these improvements may not add expenses, especially where high quality solutions reduce risks and maintenance costs. This addresses especially the problems areas of physical resilience and security and encourages spending.

3) Technical solutions need to be investigated despite the current inability of companies to invest heavily in traditional research and development. This will require considerable direct funding from government, mainly Federal, but also state. Given the current weaknesses at Lucent's Bell Laboratories as well as Telcordia and other commercial sources of telecommunications R&D, competition should be open and available to universities and small independent laboratories, commercial and otherwise. We would prefer to see increases in spending spread widely rather than focused on a small number of special institutions. The National Institute for Standards and Technology might play a bigger role, and large companies should be encouraged to collaborate through neutral bodies, but we would not wish to see the establishment of a national research laboratory. Investments should be made to ensure continued improvements to wireless technologies, especially those like the 802.11xx series of standards. Other areas for special investment might include new approaches to congestion relief, ultra wide band and spectrum switching technologies as well as voice over IP. Considerable further improvements are needed before appropriate customized content can be developed and deployed for emergency uses. This addresses many elements of the five problems areas and will stimulate business development.

4) New roles of governments and some civil society solutions

Federal jurisdiction

- Department of Homeland Security and other agencies should quickly clarify the role of secure and emergency communications and extend the Government Emergency Communications System [GETS] using wireless, IP and other modes.
- Federal mandates are need to ensure spare communications capacity set aside by service providers for emergencies. These would be emanating presumably from the Department of Commerce or the Federal Communications Commission and might be funded by something like the universal services charge. This has long been done with spare capacity requirements for port operators & shippers and for airports & airlines.
- Federally support is needed to build up special functions of local law enforcement and emergency services. Here, as in some other areas, there is need for more transfer of technology from military to civilian uses.
- Federal grant giving bodies such as the NSF and the Departments of Defense and Commerce should make resilient and emergency communications a top priority.

State jurisdiction

- Public services commissions need to take on more responsibilities for resiliency, such as the proposed New York State Public Service Commission's statutory responsibility for protecting infrastructure that would include specific requirements to maintain

vigilance in collaboration with not for profit research, professional and consumer groups and other non-commercial bodies.

- State authorities need to ensure that resiliency concerns are applied to interconnection rules and offer opportunities to experiment with different approaches.

Local jurisdictions

- Resilience associated with local economic development and the defense of local infrastructure and businesses needs to be factored in to municipal functions, as with the New York City's Department of Information Technology and Telecommunications.
- Mutual aid and restoration schemes are most important in local areas and municipal governments can encourage compliance by using their market power and through public awareness campaigns.

Civil society groups

- Voluntary action in preparation for emergencies and in times of disaster have been highly effective in solving some problems, such as using advanced communications to notify friends and family, organizing groups to respond where needed, and offering advice to those affected. We could encourage the common use of best practices for solutions such as emergency web portals [E-811], messaging systems, electronic sniffing systems (such as employed by the Wireless Emergency Response Team—WERT) and other high technology applications.
- The provision of emergency information content might best be left to civil society groups. For example, voluntary fire departments could coordinate the provision of data suitable for mobile devices to transmit emergency instructions or access special data bases relating to property, procedures, risks, etc. Some legal provision might be necessary to ensure compliance and perhaps governmental funding should be provided to meet the cost of data management.

In conclusion

We believe that addressing these resiliency concerns, although expensive in parts, will contribute overall to revenues for the communications industry. Resilience is functionality worth paying for. Furthermore, funds for homeland security are better spent in the long run in improving communications resiliency than, for example, in deploying more armed guards at unlikely targets or inhibiting international trade and travel. These recommendations will stimulate new business development and provide the means by which service providers can compete based on levels of resilience. They also ensure that innovation and variety are encouraged during this period of economic stringency for the industry.